ESD TDR 64-189
Vol I
ESTI FILE COPY

4-189

(FINAL REPORT)

THE DEVELOPMENT OF AN INFORMATION SYSTEM FOR IDENTIFICATION AND RAID RECOGNITION IN AIR/SPACE DEFENSE

VOLUME I

Initial Steps

TECHNICAL DOCUMENTARY REPORT NO. ESD-TDR-64-189, VOL. I

JULY 1963

W. S. Vaughan, Jr.
T. R. Virnelson

ESD RECORD COPY
RETURN TO
SCIENTIFIC & TECHNICAL INFORMATION DIVISION
(ESTI), BUILDING 1211

COPY NR.________ OF________ COPIES

DECISION SCIENCES LABORATORY
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
L. G. Hanscom Field, Bedford, Massachusetts

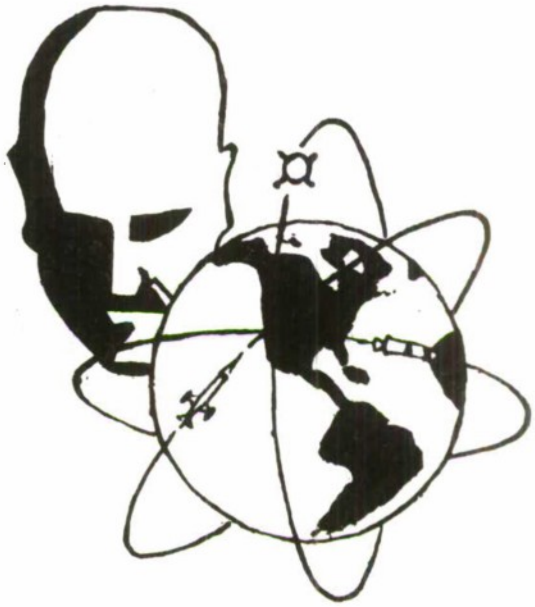
ESTI PROCESSED

□ DDC TAB □ PROJ OFFICER
□ ACCESSION MASTER FILE
□ ________________

DATE________________

ESTI CONTROL NR AL-40788

CY NR 1 OF 1 CYS



Project 4690, Task 469003

BEST AVAILABLE COPY

(Prepared under Contract No. AF 19 (628)-289 by Human Sciences Research Incorporated,
Westgate Industrial Park, Post Office Drawer 370, McLean, Virginia.)

AD 600538

When US Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Do not return this copy. Retain or destroy.

DDC AVAILABILITY NOTICES

Qualified requesters may obtain copies from Defense Documentation Center (DDC). Orders will be expedited if placed through the librarian or other person designated to request documents from DDC.

Copies available at Office of Technical Services, Department of Commerce.

ESD-TDR-64-189
Vol. I

(FINAL REPORT)

THE DEVELOPMENT OF AN INFORMATION SYSTEM FOR IDENTIFICATION AND RAID RECOGNITION IN AIR/SPACE DEFENSE

VOLUME I

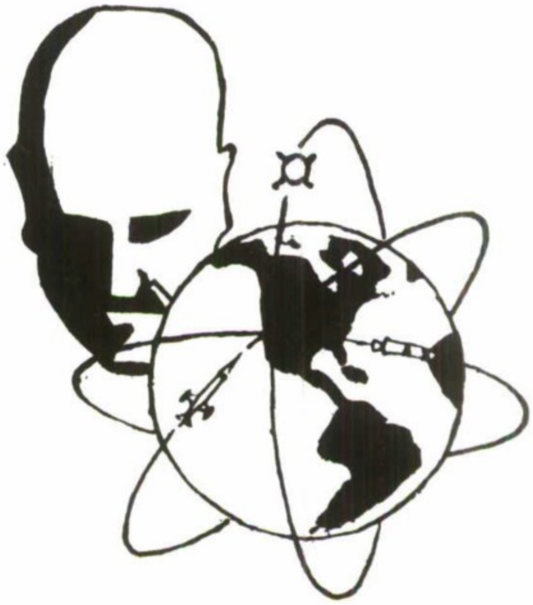
Initial Steps

TECHNICAL DOCUMENTARY REPORT NO. ESD-TDR-64-189, VOL. I

JULY 1963

W. S. Vaughan, Jr.
T. R. Virnelson

DECISION SCIENCES LABORATORY
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
L. G. Hanscom Field, Bedford, Massachusetts



Project 4690, Task 469003

(Prepared under Contract No. AF 19 (628)-289 by Human Sciences Research Incorporated, Westgate Industrial Park, Post Office Drawer 370, McLean, Virginia.)

FOREWORD

This project was initiated in November 1961 under Contract AF 19(628)-289 with the Operational Applications Laboratory, Electronic Systems Division, Air Force Systems Command. Dr. Joseph M. Doughty, then Chief, Components and Techniques Branch of OAL and now with MITRE Corporation, was the initial technical monitor. Dr. Walter E. Organist, Chief, Operator Performance Branch of OAL, later assumed monitorship of the project. Mr. Joseph T. Begley, OAL Human Factors Representative at ADC, Ent AFB, Colorado Springs, provided important liaison with ADC and NORAD military and scientific personnel.

The work of tracking down the rationales underlying some of the early development decisions in the design of identification and raid recognition in SAGE and BMEWS was done mostly through discussions with people who had a direct hand in the development process or who were otherwise aware of the reasons why a given decision was resolved in one way or another. The following people were most valuable sources of information about the early development of SAGE procedures:

Mr. R. H. Blythe, Jr., Head, Operations Analysis Group, NORAD

Dr. R. A. Jordan, Analytic Services Inc., Falls Church, Virginia

Dr. B. R. Wolin, System Development Corporation, Santa Monica, California

FOREWORD (cont'd)

Dr. J. W. Degan, MITRE Corporation, Lexington,
Massachusetts

Mr. S. J. Hauser, MITRE Corporation, Lexington,
Massachusetts

Colonel G. C. Whitley, Chief, and Captain Kyle
Delung, Directorate of Tactics and Systems
Training, ADC

LtColonel G. J. Pruett and Major R. W. Mainzer,
Systems Integration, NORAD

LtColonel N. J. Bruno, Current Operations, NORAD

The following people were the principal sources of information concerning the development of identification and raid recognition procedures in BMEWS.

Mr. R. H. Blythe, Jr., Head, and Mr. R. E.
Donegon, Jr., Operations Analysis Group,
NORAD

Mr. S. Mills and Mr. P. Gyllenhaal, RCA,
Moorestown, New Jersey

ESD-TDR-64-189

THE DEVELOPMENT OF AN INFORMATION SYSTEM FOR IDENTIFICATION AND RAID RECOGNITION IN AIR/SPACE DEFENSE

VOLUME I
Initial Steps

ABSTRACT

The system development process is an art, particularly subject to a trial-and-error kind of methodology in its early stages where functional requirements are first delineated into an approximate solution. In the present study, some specific steps in the process of developing an identification and raid recognition information system for air defense were identified and some of the considerations involved at each step were spelled out.

The development steps and the considerations they require of the developer were generalized from an examination of the evolution of identification and raid recognition procedures in SAGE, and supplemented first by the development of similar procedures in BMEWS and second by a hypothetical application of the steps to the development of similar procedures for a satellite threat environment.

Six steps are presented as a first approximation to a systematic methodology for system development as follows:

Step 1: Define system response levels.

Step 2: Define air/space threat levels.

Step 3: Develop and time sequence identification and raid recognition techniques.

Step 4: Reduce threat levels to a practical number of categories.

Step 5: Match system response levels (1) to threat levels (4).

Step 6: Specify criteria for accepting presence of threat levels.

Publication of this technical documentary report does not constitute Air Force approval of the report's findings or conclusions. It is published only for the exchange and stimulation of ideas.

Herbert Rubenstein

HERBERT RUBENSTEIN
Chief, Decision Techniques Division
Decision Sciences Laboratory

ROY MORGAN, Colonel, USAF
Director
Decision Sciences Laboratory

KEY WORD LIST

1. COMMAND & CONTROL
2. IDENTIFICATION SYSTEMS
3. DATA PROCESSING SYSTEMS
4. DECISION MAKING
5. SATELLITES (ARTIFICAL)
6. DETECTION
7. EARLY WARNING SYSTEMS
8. DEFENSE SYSTEMS

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

LIST OF TABLES AND FIGURES

SECTION 1
INTRODUCTION

Problem Area and Study Purpose

The development of semi-automated information systems for command and control is usually initiated by a statement of functional requirements which must be satisfied, and has as its end product an operational system-in-being. The resulting system is a complex of equipment, operators, procedures, and statements of doctrine. which govern the conduct of procedures. In the U. S. Air Force, requirements for system development are contained in Specific Operational Requirements (SORs) which express in functional terms the needs to be satisfied by the system. The process of bringing about an operating system is the responsibility of a System Project Office (SPO).

The system development process is a methodology, essentially a series of steps or decisions, for translating an expression of a functional need into a system-in-being. For the most part, the process of system development is a not-well-understood art -- no explicit statements of how-to-do it exist. This lack of systematic procedures is particularly noticeable in the early stages of system development where the expression of functional need is initially reduced to a concept of how the requirements will be solved. In later stages of system development, where problems such as man-machine task allocations and operator-console interface relationships must be solved, some guidance is available to system developers in the form of data descriptive of human capabilities to read displays, discriminate auditory signals, reach various distances, apply certain forces, etc. At the level of initial conceptual delineation of a complex functional requirement into a general structure of a solution, however, there are no similar handbooks and few articulated principles or guidelines which the system developer can systematically apply.

The purpose of the present study was to take an initial step towards specifying a methodology and providing a set of guides to structure the early stages of future system development. This report contains the unclassified description of the methodology. Volume II, under separate cover, contains the classified information on identification and raid recognition techniques used as a basis for this report.

Scope and Approach

A limited portion of an air/space defense command control system, the identification and raid recognition subsystem, was selected as the scope of the study. Identification and raid recognition subsystems had been developed in an aircraft threat environment as part of SAGE and in a missile threat environment as part of BMEWS. Therefore, two reference systems-in-being were available for study. This selection was further compelling since a similar subsystem would eventually need to be developed for a satellite threat environment and any useful guides to development produced by this study might find application there. Furthermore, only the pre-war, early warning functions of the identification and raid recognition subsystem were analyzed. The pre-war environment was chosen as the context for study since it has been the most prevalent condition of the past, therefore most of the system development experience has been in this context, and it is the condition most likely to continue in the future.

The approach used in this study was to trace the development of identification and raid recognition procedures in SAGE and BMEWS in order to abstract, from the rationale involved in their development, generalizations about the conduct of the initial stages of the development process. These generalizations were supplemented by information about how the development steps might be applied in a hypothetical satellite threat environment. Finally, six steps in the initial development process were specified as a first approximation to a systematic methodology and guidelines for their application were drawn from all three sources.

Definition of an Identification and Raid Recognition Procedure

Identification is the process of resolving the threat status of individual air/space borne objects detected. Raid Recognition is the process of estimating the likelihood that the presently known state of air/space activity includes an enemy air/space borne attack. These two processes are carried out continuously in an air/space defense system as a means for providing tactical early warning of an attack. The basic components of the procedure by which identification and raid recognition processes are conducted consist of a set of techniques which test information about a detected object or test information about the overall state of air/space activity for level of threat. Each technique includes criteria against which the received information is compared in order to accept or reject the threat condition tested for. The outcome of the application of an identification technique is a classification category describing the threat status of the object tested. The outcome of the application of a raid recognition technique is an alarm level or a classification category indicating the likelihood that the present level of air/space activity could occur by the presence of non-threatening events only. Each level of individual or overall threat state, described in a shorthand manner by the use of classification categories or alarm levels, implies the necessity for an appropriate level of response from the defense system facilities. Finally, the techniques are applied in sequence, the order of which is determined by the outcomes of the previous technique and the availability of information required by each technique.

Definition of the components of an identification and raid recognition procedure suggests ways in which the development of techniques and criteria are influenced by such considerations as available system responses, anticipated types and levels of threat, the availability and reliability of information. The second and third sections of the report present and illustrate the specific ways in which these and other considerations influence the development of information systems for air defense. Section 4 presents a distillation of these examples into six development steps and guidelines for their resolution and implementation.

SECTION 2

GENERALIZATIONS ABOUT SYSTEM DEVELOPMENT FROM SAGE AND BMEWS

Threat States and System Response Levels

Before the development of identification and raid recognition procedures for a particular system can begin, it must be decided what states of individual objects the system should be able to "identify" and what states of the overall situation the system should be able to "recognize. Resolution of these decisions requires a consideration of available system responses since the reason for performing identification and raid recognition is to enable the system to make the responses at its command at appropriate times. Ideally, it would be determined what state of the environment was sufficiently threatening to warrant the use of each available response. Each of these threat states would be described in terms of quantities which the defense system could observe and measure, thereby making it possible for the system to "identify" or "recognize" each state when it arises. Each of these states, which define the range of interest of the identification and raid recognition functions, would be given a short label. Each short label would be the prescribed signal for the appropriate response.

Under these ideal conditions, when the threat evaluation portion of the defense system would detect a defined threat state, it would signal the response control portion of the system using the detected threat state's short label, and the response control portion would make the appropriate response.

Responses can be divided into two groups: those responses made to states of a single object and those made to overall threat states. System responses to states of individual objects are typically actions to obtain new information, to conduct additional processing with information already available, or some attempt to alter the object's behavior. Responses to the overall air/space situation are principally preparations for active and passive defense and preparation for retaliation.

To date, it has not been possible to specify in operational terms the states which must exist before all responses will be employed. Three factors appear to be determining considerations in whether a threat state can be specified for a response. One is the reliability of the data on which the likely choices for threat state would be diagnosed, the second is the severity of the consequences of the response, and the third is time-to respond limitations. In general, where the reliability of the data base used is low and the response is one with severe consequences and there is time to consider other factors, the decision will be left to the tactical judgment of a responsible commander. Where the reverse conditions obtain, a threat state sufficient to warrant the response will be specified. It is with the intermediate cases where the system developer's problem becomes difficult. In the case of BMEWS for example, the data base used for raid recognition is not free from error and some false alarm probability exists, the appropriate responses to an alarm are rather severe (if in fact no raid is in progress, the responses may provoke one), but the time for judgment is very limited. It appears that some intermediate solution is feasible. Some responses, particularly those internal to the system, could be made as a matter of doctrine while reserving to judgment, decisions about responses whose effects are external to the system.

Threat states warranting responses to individual objects tend to be specified, while threat states warranting responses to the overall threat state tend to be left to the discretion of the military commander. In the development of identification procedures in SAGE, for example, discrete stages of threat for individual objects were defined, labeled, and an action prescribed as the system's response. The label served, at once, to identify a threat state and to specify the required response. The designed progression of threat state--label--response is illustrated in Table 1.

In the case of responses to the overall situation, warranting threat states have not been described in operational terms. In current NORAD operations, there are six levels of defense readiness (Defense Conditions) and seven levels of weapon preparedness (Weapons Control Cases).[1] Threat states sufficient to warrant these responses have not been described in operational terms. However, certain relevant characteristics of the overall situation are recognized. Examples of these characteristics are number of UNKNOWNS in SAGE and probability that BMEWS has detected an ICBM attack. When SAGE UNKNOWNS exceed a certain level, the air defense commander is notified. With increasing levels of confidence that BMEWS has detected a missile attack, BMEWS ALARM LEVELS are generated for the air defense commander. Whereas no responses are by doctrine automatically made solely on the basis of this information, number of SAGE UNKNOWNS and BMEWS ALARM LEVELS are important factors in determining when responses to the overall situation are made.

[1] Simulated Defense Readiness Conditions, Air Defense Warning and Weapons Control Cases. NORAD Regulation No. 55-1. Headquarters North American Air Defense Command, Ent AFB, Colorado. 24 January 1961.

TABLE 1

Threat States, Labels, and Prescribed Responses in SAGE Identification Procedures

THREAT STATES	THREAT STATE LABELS	SYSTEM RESPONSES
Detected object is an aircraft and must be identified with respect to threat	PENDING	Apply identification techniques
Aircraft satisfies a criterion for non-threatening (criteria in terms of such measurable quantities as object's speed)	FRIENDLY	Monitor parameters on basis of which aircraft was accepted as non-threatening
Aircraft cannot be identified by techniques based on routine surveillance system	UNKNOWN	Launch a non-routine surveillance device (interceptor) for additional information
Aircraft satisfies a criterion for threatening	HOSTILE	Destructive action is initiated

Threat states, labels, and responses for NORAD raid recognition, utilizing information from both SAGE and BMEWS are shown in Table 2.

As contrasted with identification procedures (Table 1), the first column in Table 2 contains only indications of threat states rather than definitions. There is no explicit rule tying the presence of a condition listed in Column 1 to the Threat State Labels of Column 2. Conditions such as the occurrence of an alarm level is only one consideration in the commanders tactical judgment of the nature of the present threat state. Also in contrast to identification procedures, the labeling of a threat state does not specify the appropriate system response. Sets of responses are grouped together as a DEFCON, but under what conditions a given DEFCON is ordered, again is a matter of judgment rather than doctrine.

TABLE 2

Threat States, Labels and Responses in NORAD Raid Recognition Procedures

THREAT STATE INDICATORS	THREAT STATE LABELS	SYSTEM RESPONSES
Critical number not exceeded (SAGE) Alarm level thresholds not exceeded (BMEWS) Critical number exceeded (SAGE) Alarm level thresholds 1, 2 or 3 exceeded (BMEWS)	Air Defense Warning WHITE (air attack is improbable) Air Defense Warning YELLOW (air attack is probable) Air Defense Warning RED (air attack imminent)	Weapon Control Case 1-7 Defense Condition 5-1 Air Defense Emergency

Techniques and Criteria for Identification

Four general techniques for the identification of individual objects with respect to threat can be abstracted on the basis of SAGE and BMEWS experience. Each technique is defined in terms of the classes of information about the detected object which are used. In this section, each technique will be described in terms of the procedure used for identification, the conditions which must be satisfied in order to use the technique, and the problems of criterion development associated with its use.

Trajectory Characteristics

Description and Requirements. This technique is used in both SAGE and BMEWS for the positive identification of non-threatening events. The principal function of the technique is to quickly reduce the number of detected events which must be processed for identification by more expensive techniques later in the sequence. For example, in SAGE, all aircraft detected whose airspeed is below a specified value are classified as FRIENDLY and monitored, but no additional identification techniques are applied. In BMEWS, a detected object whose predicted impact location is outside of defined geographical boundaries is removed from further processing.

The general procedure involved is to match computed characteristics of the object's trajectory against stored limits, values, categories, ranges, etc., which have previously been determined to satisfy criteria for the definition of a non-threatening event. Two conditions must be satisfied for this kind of technique to be applicable in identification:

The definition of a non-threatening object includes values of one or more trajectory characteristics as a sufficient condition.

Relevant trajectory parameters can be calculated within useable accuracy limits from data obtained by the surveillance system.

Criterion Development. The crucial system development decision in the use of the trajectory characteristics technique is the selection of criterion values or ranges of values on the trajectory parameters involved in the definition of non-threatening. These values operationally define "non-threatening." In SAGE, for example, airspeed was determined to be a trajectory parameter which could be used to discriminate non-threatening from potentially threatening aircraft--those aircraft with airspeed values in a low range were unlikely to be armed bombers on an attack mission. The selection of the boundary value of airspeed required the system developer to take an explicit trade-off position between the risk of classifying as FRIENDLY a truly threatening aircraft and the risk of overloading the processing system at the next technique in the sequence. The first risk is based on the probability of an enemy attack bomber operating at an airspeed within the criteria for non-threatening. The latter risk is a function of a man-machine design parameter: the capacity of facilities planned for the next step in the identification process. In SAGE, the next technique required operators to match computer-stored flight plans with sensed-data trajectories projected on a display face. Number of tracks which could be correlated was limited by computer storage space available, display limitations and time required for operators to perform the matching operation.

The selection of criterion values, therefore, involves several considerations which define the trade-off between two risk probabilities and the consequences of those risks. The probability of misclassifying an enemy bomber as FRIENDLY is essentially zero if the boundary value on airspeed is set at or below stall speed of the reference aircraft. As the criterion value is increased, increased numbers of slow flying, small, privately operated aircraft can be classified FRIENDLY and removed from further processing at the cost of some increment of risk of misclassifying an enemy bomber. In the early development of SAGE, a very conservative value of airspeed was used as a criterion, few flights could be identified FRIENDLY by this technique, and the system experienced an overload at the next processing technique in the identification sequence, which resulted in essentially no further processing. The criterion was relaxed, the system developers accepting a slightly increased risk of missing an enemy bomber for the gain of an operating system.

The following general steps can be defined as a procedure for developing criteria for the trajectory characteristic technique:

Identify trajectory parameters provided by the surveillance system.

Plot the distributions of values on these parameters for non-threatening objects.

Plot the distributions of values on these parameters for potentially threatening objects.

Determine if a sub-range of values exists which is more typical of one distribution than the other. Select the limits of the sub-range as criteria in such a way as to achieve a best balance between the risk of overloading the processing system by identifying too few friendly objects and the risk of reducing sensitivity of the technique to threatening objects. Any object exhibiting a value in the sub-range defined by the criteria will be classified threatening or non-threatening as the case may be.

Correspondence Between Sensed and Planned Characteristics

Description and Requirements. A version of this technique (flight plan correlation) is used in SAGE for the positive identification of non-threatening aircraft. This step serves to further eliminate aircraft from threat processing by later, more expensive techniques. Certain characteristics of the aircraft's actual flight path are computed from sensed data and compared with the planned values. If the aircraft's sensed characteristic is within limits defining correspondence between the planned and sensed values, the aircraft is identified as FRIENDLY. No technique similar to this is used in BMEWS.

The general use of this technique could be expanded to include other than trajectory characteristic matching. Planned values on physical characteristics could be sensed and compared with planned values. The following conditions are required:

> Non-threat character of the object can be assured prior to its launch but surveillance system cannot track the object continuously from point of launch.
>
> Continuous tracking of the object can be performed by the surveillance system at some period of time after launch.

> There are communication facilities for transmitting planned trajectory and physical characteristics information and changes thereto to the air defense system.
>
> There are facilities whereby deviations from planned values can be detected by object's controller (pilot in the case of manned vehicles).

Criterion Development. Two kinds of criteria are needed in order to implement the Correspondence technique. The first criterion required is a definition of a non-threatening plan and the second is a definition of correspondence. With these two criteria developed, a submitted plan can be compared to criteria for non-threatening and judged to satisfy or not satisfy them; then, if the plan is not threatening, detected characteristics of air/space activity can be compared with planned characteristics and judged to correspond or not correspond on the basis of the second set of criteria.

In SAGE, criteria defining "friendliness" of a submitted flight plan were not made explicit. Practically all plans filed with FAA's Air Movements Identification Section (AMIS) were for routine commercial flights of obviously friendly nations into U. S. airports. Non-routine plans were referred to the Department of State and possibly to the Joint Chiefs of Staff for a ruling on the political and military advisability of allowing the flight.

Criteria for defining correspondence between sensed trajectory information and plans are explicit in SAGE. They consist of lateral position error limits in terms of miles, and longitudinal position errors in terms of time.

Three types of considerations in developing criteria for a non-threatening plan can be identified from individual examples of rejected flight plans in SAGE. These are the capability of the object to conduct threatening missions, the proximity of the flight to areas defended by the U. S., and the inferred intent of the object's controller based on the political relationship between the U. S. and the nation submitting the plan. Criteria which vary in level of conservatism may need to be developed for plans of nations of varying degrees of political friendliness.

Two kinds of considerations must be taken into account in the development of criteria for correspondence. One is the rate at which the criteria will generate non-corresponding events; the second is the nature of the response planned for such events. Given a rate of occurrence of events to be processed by this technique and an empirical distribution of error magnitude on the characteristics used to define correspondence, then any set of criterion values selected will yield an average rate of non-corresponding events over a fixed time interval. This rate can be calculated for various combinations of criterion values or a rate limit can be specified and values computed which will result in the specified rate. If the response to non-corresponding events has a limited rate, then the selection of criterion values for defining correspondence should be constrained by this rate. This is the case in SAGE where interceptors are scrambled against non-correlating aircraft. Interceptors available, turn-around time required, etc., specify a maximum average scramble rate. Criteria for correspondence must be sufficiently broad so that this average rate is not exceeded by the average rate of events requiring the response.

The following general procedure is used to select criteria for correspondence:

> For each characteristic, plot distribution of error between sensed values and corresponding values from filed plans.
>
> Restrict the selection of values on the characteristics to those which yield a rate of non-corresponding events which is equal to or less than the maximum response rate of system facilities planned for use.

Authenticating Response to Interrogation

Description and Requirements. This technique has been used in SAGE for the positive identification of non-threatening aircraft. Parts of the Multiple Corridor Identification System (MCIS) procedure included a radio response to a radio interrogation, a check turn response to a radio interrogation, and a more complex maneuver response to a radio interrogation. These procedures were used to further reduce the numbers of unidentified aircraft which had to be intercepted for visual identification. Electronic Identification Friend or Foe (IFF) developments are also considered an example of this general technique. The Mark X SIF equipment system includes a radar interrogation of an airborne transponder with three response codes which identify three types of aircraft: commercial traffic, SAC bombers, and interceptors. Mark XII - Mode 4 development includes a computer-generated cryptographic code which increases the security of the previous system.

The general procedure of this technique is to prearrange, between the system interrogating element and the friendly aircraft responder (pilot or transponder), a coded interrogation and response which defines non-threatening aircraft. If only pilots of friendly aircraft know the correct response to the interrogation and the response is both easily discriminated from routine behavior and secure from enemy imitation, then aircraft exhibiting a correct response to interrogation are friendly. The following general assumptions are required for the successful development of a technique of this type:

> There is a means for communicating interrogations to individual air/space borne objects.
>
> The object itself or equipment mounted in the air/space borne object can perform a range of responses, one of which can be defined as an authentication of its identity as a non-threatening object.
>
> There is a means for the response to be communicated to the interrogator in such a way that the response can be associated with the object.
>
> There is a means for comparing the response with a definition of a correct or authenticating response.
>
> The response is secure from enemy interference or copy.

Criterion Development. Historically, the major problems in the development of the Authenticating Response technique have been with satisfying the basic requirements other than criterion development. Radio responses failed since direction finding equipment could not accurately localize the source of the transmission. Check turn and other maneuver responses were often not easily recognized from radar traces on a PPI scope. Electronic solutions have experienced problems of security from copy and interference from ECM.

To the extent a technique of this type might be contemplated for future development, the central criterion problem to anticipate is in the definition of a "correct" response. The extent to which an actual response must approximate the required response in order to be identified as non-threatening will have to include such considerations as noise levels in the type of channel over which the interrogations and responses are communicated, the reliability and error rates of the equipment involved, and the nature of the system action planned in the event no response or an "incorrect" response is received.

Physical and Behavioral Characteristics

Description and Requirements. Information about a detected aircraft's physical characteristics and airborne activities has been used in SAGE as a basis for the positive identification of threatening as well as of non-threatening aircraft. Visual acquisition of the detected aircraft by the interceptor pilot provides much more information about the aircraft than is contained in its trajectory parameters. The capabilities of the aircraft can be inferred from its silhouette. A military aircraft with externally mounted missiles is unmistakably capable of destructive action. Its silhouette and markings also provide a reliable cue to the nation which ordered its mission. If the aircraft exhibits behavior preparatory to the delivery of a bomb or missile or commits other acts indicating a hostile intent, these behaviors can be used as a basis for a reasonably certain inference of hostile intent.

Successful development of this type of identification technique assumes the following general conditions are met:

> Information is available about physical or behavioral characteristics of the air/space borne object other than trajectory.
>
> One or more of the physical or behavioral characteristics is included as a sufficient condition defining a friendly or a threatening object.

Criterion Development. Criteria are needed to define, on the basis of sensed physical and behavioral characteristics, a non-threatening object which can be classified FRIENDLY and assigned to routine monitoring, a threatening object which can be classified HOSTILE and destroyed, and intermediate levels of ambiguity of threat which require intermediate responses. In SAGE, criteria are made explicit for the classification as HOSTILE and it is assumed that a U. S. commercial airliner and other aircraft of approximate non-threatening character will be classified FRIENDLY. No criteria are spelled out, however, for mixtures of inferences of capability and intent which are of ambiguous threat. The nationality of the aircraft, inferred from silhouette and markings, may be friendly, but the capability clearly military and the proximity to U. S. defended areas rapidly increasing. Or the nationality may be one clearly at odds politically with the U. S. and a destructive capability cannot clearly be ruled out, and the range to U. S. coastline is closing. In the absence of doctrine these cases are responded to on the basis of the tactical judgment of the responsible Commander.

The major consideration in the selection of criteria is the severity of the system response planned. In SAGE the response to an aircraft classified HOSTILE was its destruction. Since this was a most extreme act, it was determined to be warranted only if the aircraft in question committed an act so obviously aggressive as to provide unquestionable evidence of a hostile intent. Consequently, criteria for a HOSTILE classification are very conservative. Less severe responses might warrant less conservative criteria.

General procedures for developing criteria are as follows:

Determine distributions on detected physical and behavioral characteristics for threatening and non-threatening air/space borne objects.

Determine a sub-range of values on these characteristics which define non-threatening objects at an acceptable level of risk of misidentification.

Determine a sub-range of values on these characteristics which define, at a specified level of confidence, an object sufficiently threatening to warrant its destruction.

Determine additional intermediate sub-ranges of values for as many intermediate levels of response as are available between assigning the object to routine monitoring or destroying it.

Techniques and Criteria for Raid Recognition

Two general types of raid recognition techniques have been developed in SAGE and BMEWS. The first is based on the number of detected events in a limited time interval or the number of simultaneously occurring events whose threat status cannot be resolved by routine processing. The second technique is a refinement of the first in that certain characteristics of the events are weighted as a function of their value.

Critical Number

Description and Requirements. This technique was used in SAGE for the purpose of early warning when the first tactical information about incoming aircraft came from the perimeter radar systems. The number of detected aircraft which could not be identified non-threatening on the basis of routine identification techniques, but turned out to be friendly upon visual acquisition, was used as an empirical base for defining normal conditions. This number varied in magnitude with traffic volume which in turn was a function of time of day, day of week, season of year and geographic area. A critical number was selected as a threshold for various regions, times of year, days of week, and hour of day to statistically define a significant increase in unidentified traffic. Later, with the development of more distant early warning radar picket lines such as Mid-Canada, Pinetree, and Mid-Atlantic, this technique was adapted to numbers of aircraft penetrating the radar fence of defined length over fixed time intervals.

The following conditions are assumed in the development of the critical number technique for raid recognition:

In normal conditions of air/space activity, there will occur some average number of detected events, which cannot be identified non-threatening.

In an air/space borne attack condition, this average number will be significantly exceeded.

Factors, which systematically influence the magnitude of the number of events other than the presence of an enemy raid, are known.

A criterion for defining "significantly exceeded" can be developed.

Criterion Development. The key decision in the development of this technique is the selection of a threshold value or number which will define a non-normal condition of air/space activity. Selection of the threshold value specifies a position on the trade-off between sensitivity to raids and probability of a false alarm. As the threshold is set lower to detect smaller raid sizes, the likelihood of the threshold being exceeded by normal events is increased. Empirical data, gathered over recent time intervals, can be used as a base for calculating the trade-off consequences of selecting various values as threshold.

The selection, therefore, is a matter of judgment involving two general considerations: how small a raid size must the technique detect, and what is the limit of an acceptable false alarm rate. The sensitivity consideration involves questions of the amount of damage which could be inflicted by an attack of various numbers of aircraft, missiles or whatever air/space objects are of concern, and the amount of damage the U. S. should tolerate before confirming that an attack is in progress. The consideration of acceptable false alarm probability involves the question of the nature of the system responses planned in the event threshold value is exceeded. To the extent that responses are internal to the system (alerting operational personnel, increasing numbers of defensive weapons on advanced readiness conditions, etc.), costs are in terms of dollars and loss of availability of some portions of the defense system facilities for some time interval while refueling, maintenance, etc., is performed. These costs are mitigated by the value of system exercise in training operators, diagnosing system weaknesses, and testing new procedures or equipment. To the extent that responses will require external activity such as control over commercial and civilian activities, launching defensive weapons to orbit points, or committing offensive weapons, then costs are increased to include risks of civil panic and unwarranted provocation of the opponent.

General procedure for developing a threshold value for this technique is as follows:

Tabulate frequency of occurrence of non-threatening objects detected and unresolved by identification techniques.

Determine factors other than presence of enemy raid which influence the frequency of occurrence.

Determine an acceptable false alarm probability on the basis of size of raid to be detected and cost of responses planned.

Calculate the threshold number which will be exceeded at the accepted false alarm rate for as many non-raid conditions as influence the number of non-threatening objects.

Critical Weight

Description and Requirements. This technique was developed in SAGE as a refinement of the critical number technique. The purpose of the refinement was to simultaneously increase sensitivity to raid-like events and decrease false alarm rate. This was accomplished by assigning different weights to non-correlating aircraft on the basis of its speed and altitude. Those speed and altitude values which typically occur in non-correlating friendly aircraft were weighted less than those values of speed and altitude which were atypical. A weighting technique is also used for raid recognition in BMEWS. Weights are assigned on the basis of the reliability of the data about the detected event. Two categories of reliability are available with data from the search radar: a one-fan event is of low reliability, a two-fan event is of high reliability. This difference is accounted for in two ways: first the high reliability events are heavily weighted compared to the low reliability events; and second, a limit is placed on the amount of weight which low reliability events can contribute to the total weight representing the overall threat situation. In both systems, the total weight from detected events is compared to one or more threshold values selected as criteria for air/space activity beyond normal levels.

The following conditions are required for the development of a critical weight raid recognition technique:

One or more bases exist for scaling the degree of threat posed by objects which cannot be identified non-threatening by identification techniques.

In normal conditions of air/space activity, there is an average overall weight which results from summing over characteristics of all detected objects not eliminated as non-threatening.

In conditions of air/space activity which includes an air/space attack, the overall weight will significantly exceed normal.

A criterion can be developed which quantitatively defines "significantly."

Factors which influence weights and are non-raid related have been identified and accounted for.

Criterion Development. The criterion problem in the development of this technique is essentially the same as that described for the critical number technique. The selection of a threshold value specifies a known level of raid detection sensitivity and a false alarm probability. In the solution to the criterion problem developed in BMEWS, three refinements in selecting threshold values were made. First, since a raid could pass through the detection radar fans in different time distributions, threshold values were calculated for three different time intervals representing reasonable ways the enemy might spread or concentrate his attack in time. Second, since a raid could pass through the detection fans in different spatial distributions, thresholds were calculated for each of three areas along the line. Third, since levels of response varied in severity, threshold values were calculated for three different false alarm probabilities. These threshold values represent increasing degrees of confidence that events other than normal activity have occurred.

General steps in the development of criterion weights are as follows:

Tabulate frequency of occurrence of weights resulting from non-threatening objects which cannot be identified by identification techniques.

Determine and account for factors other than presence of enemy raid which influence distribution of weights.

Determine several likely temporal and spatial distributions of enemy passage through surveillance coverage.

Calculate several critical weights as threshold values which reflect increasing confidence in presence of a raid and which reflect sensitivity to raids of different temporal and spatial concentrations.

Sequence of Application of Techniques

Techniques for identification and raid recognition must be applied in some temporal order. Where several criteria can be used as tests for threat with a given technique, then the order of tests within a technique also must be planned by the system developer.

Sequencing decisions involve considerations of cost and effectiveness in reducing the ambiguity of the threat status of the individual object or overall air/space situation. Cost considerations involve both the time and facilities required to obtain and process the necessary information. Effectiveness is essentially the power of the test in resolving the threat. The most powerful technique is one whose application produces a positive identification of threatening objects. The next most powerful technique is one which positively identifies non-threatening objects, since these objects can be subtracted from the total air/space activity requiring further processing.

The sequence of application of techniques in SAGE and BMEWS is on the basis of minimizing cost. Information from the routine, continuously operating surveillance radars is processed first with a trajectory characteristic technique. Next in the sequence are those techniques which require information in addition to that provided by radar such as flight plan correlation and the Multiple Corridor Identification System. Both of these techniques require additional sources of information, communications and data processing. The last technique for identification in SAGE is also most expensive, requiring the scrambling of an interceptor to perform visual identification. The same principle is used in BMEWS: tests requiring the most simple data processing are made first.

Total time available for data processing of this sort can be defined by reference to a maximum time delay. This allowable time delay is based on a consideration of time factors associated with speed of incoming aircraft, detection range, range to bomb release line, time required to scramble interceptor and intercept target.

In summary, the following generalizations can be made regarding sequencing of decisions:

> Use techniques in the order of their cost, considering availability of information about detected objects and data processing requirements of the technique: least expensive techniques first.
>
> Use a positive test for threatening objects at the earliest opportunity.
>
> In the absence of tests for threatening objects, use tests for non-threatening.
>
> Use a raid recognition technique when all tests for non-threat have been applied and objects of unresolved threat status remain.

SECTION 3

INFORMATION SYSTEM DEVELOPMENT IN A SATELLITE THREAT ENVIRONMENT

In the development of a system to assess the threat of and control responses to enemy satellites, the decisions discussed in Section 2 will have to be resolved. In this Section, some considerations involved in resolving these decisions for such a system are discussed. The assumed satellite threat environment is based on material in the references listed in the Appendix. Responses which likely will be available and threat states warranting their use are indicated. Then, techniques for detecting these threat states and the likely sequence for applying these techniques are discussed.

Threat States and System Response Levels

There will be many responses available for use against the overall satellite threat environment. These responses will include such things as increasing readiness of defensive and offensive forces, hardening and deploying offensive and defensive forces, reducing vulnerability of the civilian population, and employing offensive and defensive forces. It is likely that, as in the past, threat states warranting the use of these responses will not be defined in operational terms.

Five responses used against individual objects in the past appear likely to be used against satellites.

Gather Information With Continuously Operating Surveillance Devices

Radar, optical telescopes, RF intercept equipment, and IR sensors will be capable of operating continuously and will all provide information about trajectories of satellites. Rough measurements of size, shape, and stabilization may be available from these sensors. This response would be made continuously as long as there is some possibility of an air/space attack against the U. S.

Gather Information With Non-Continuously Operating Surveillance Devices

Mass sensors, nuclear materials sensors, optical imaging equipment, photographic equipment, and RF intercept equipment mounted on a rendezvous-type vehicle will be able to make short-range measurements on satellites. Because of cost considerations, the rate at which these vehicles could be employed would be limited. The sensors listed above would provide information about different characteristics (mass, presence of nuclear materials) of the satellite than would continuous surveillance; they would also provide finer information about the same characteristics (size, shape, stabilization, etc.) as continuous surveillance. This response has been used in the past whenever the system was unable to identify an object as non-threatening on the basis of information provided by the continuously operating surveillance devices. In SAGE, there was a limit on amount of time which could be spent processing data from continuous surveillance before this response was taken. Some kind of time limits will probably be specified for satellite identification also.

Bring a Destructive Weapon Within Range of the Object

In addition to sensing devices, the rendezvous-type vehicle will mount a weapon capable of destroying a satellite. The vehicle can be deployed into an orbit sufficiently close to a suspicious satellite that the satellite is within effective range of its weapon. This deployment obviously decreases the time required to destroy the satellite if this action becomes necessary. Because the destructive weapon and secondary surveillance devices are mounted on the same vehicle, this response and the previous response are made simultaneously.

Communicate a Request to the Object's Controller to Reduce Threat Status

The U. S. will be able to communicate with the countries likely to have placed a particular satellite in orbit via either a "hot line" or normal State Department channels. It may happen that the launching country could explain away any threatening appearance of the satellite or could cause the satellite to take some action which would reduce its threatening appearance. This response would probably be made if the system was unable to identify a satellite as threatening or non-threatening after using all possible surveillance devices.

Destroy Object

A rendezvous vehicle mounting an anti-satellite weapon and already in orbit close to a threatening satellite could destroy the satellite in a matter of seconds. In SAGE, destructive action would be taken whenever, and not until, an aircraft evidences a hostile intent by taking some observable, unmistakably aggressive actions against the U. S. In the future it must be decided what conditions must arise before destructive action will be initiated against a satellite, assuming such a capability exists. It may be that a nuclear emission level and a mass typical of a nuclear warhead would be considered sufficient grounds for destructive action. Possibly, conditions on the satellite's orbit would also have to be satisfied. Specification of the conditions sufficient to justify destructive action will be an important step in the development of an identification procedure against satellites.

Techniques and Criteria for Identification

So that the anti-satellite defense system can appropriately make the responses just discussed, the system will employ identification techniques to detect the threat state warranting each response. Of course, before any techniques can be selected for use, there must be operational definitions of which detected satellites will be destroyed (threatening satellites) and which can be eliminated from testing by further techniques (non-threatening satellites). Once these definitions are made explicit, conditions warranting the responses become easily recognizable by the system.

Trajectory Characteristics

The information about detected satellites which is most quickly and cheaply available today is trajectory information. Consequently, it would be of great advantage if the Trajectory technique could be used to identify satellites. This technique would involve a comparison of the observed orbital elements of a satellite's trajectory with established criteria for a non-threatening trajectory.

This technique would be possible only if the U. S. had included in its definition of a non-threatening satellite or of a threatening satellite at least one case involving only trajectory characteristics. For example, any synchronous satellite stationed beyond missile range of the U. S. might be defined as non-threatening. Or, any satellite whose perigee exceeded some minimum value might be defined as non-threatening.

In order to select the criteria to use with this technique, two distributions, one empirical distribution for non-threatening satellites and one estimated distribution for threatening satellites, are plotted for each trajectory characteristic. Typical plots might be made, for instance, for inclination, eccentricity and perigee. The two distributions for each characteristic would then be examined to see if some range (or ranges) of values on the characteristic is more typical of one distribution than the other. If there is such a range, values defining the limits of the range would be selected taking into account losses due to threatening satellites identified as non-threatening and to increased numbers of unidentified satellites. Any satellite exhibiting a value in such a range is classified threatening or non-threatening as the case may be.

Correspondence Between Sensed and Planned Characteristics

Another identification technique using orbital elements calculated from observed orbit data is available. This is the Correspondence technique in which the observed orbit data is compared with data on non-threatening satellites in established orbits or data onplanned launches of non-threatening satellites. If the difference between the observed data and the established or planned orbit is within tolerance limits defined by criteria for correspondence, the object is classified as non-threatening.

A defense system whose surveillance tracked satellites continuously from the time of launch to the moment of re-entry would require flight plans only on satellites launched from neutral or non-friendly areas. It could be assumed that any object launched from a friendly area would be non-threatening. Also, there would obviously be no need for correlation with established orbits if tracking were continuous.

A defense system whose surveillance could not track satellites continuously from launch would not know, relying on surveillance information alone, where a newly detected satellite had been launched from. It could not, therefore, identify satellites launched from friendly areas as non-threatening on the basis of launch area. Consequently, to identify these satellites, the system would require launch plans from friendly areas as well as from neutral and non-friendly areas. Also, since detected satellites could not be tracked continuously, the system would have to reidentify each satellite each time it reappeared. Consequently, tests for correspondence with established orbits would be made.

It can be seen that launch plans (including description of planned orbits), received in advance of launch, could be of assistance in the identification of satellites. Friendly flight plans would be supplied to the defense system as matter-of-course. If in the future the U. S. develops an effective anti-satellite weapon, politically neutral and unfriendly nations may also supply the U. S. space defense system with launch and orbit plans, lest their scientific and commercial satellites be mistaken for military vehicles and destroyed.

Of course, the mere reception of launch and orbit plans would not insure a non-threatening mission. If the U. S. definition of non-threatening satellites specifies that certain orbits are sufficient in themselves -- without respect to the nature of the vehicle -- for identification as non-threatening, received plans could be checked to see if the planned orbit is a non-threatening one. If so, then if the detected satellite conforms to the non-threatening orbit, the satellite itself can be classified as non-threatening. In this case, the correspondence technique would reduce to the trajectory technique. However, if there are no orbits sufficient in themselves for classification as non-threatening, or if there are non-threatening orbits but the planned orbit is not one of them, then the vehicle itself would have to be considered.

The launching nation might include in the plan details about the vehicle (such as size and mass) which could be verified by U. S. surveillance after launch. If the U. S. definition of a non-threatening satellite were to include criteria such as low mass or small size, the plan could be checked against these criteria to see if it could be classified non-threatening. If it could and if a detected satellite conforms to the plan, the satellite itself could be classified non-threatening. In this case, the correspondence technique would reduce to the Physical/Behavioral technique.

If there is insufficient information in a received plan to permit classification of the plan as non-threatening, the U. S. might request some form of inspection of the vehicle on the pad before it would classify the plan non-threatening and withhold destructive action.

Criteria for correspondence will have to be established. These criteria will specify how closely a detected object must conform to a non-threatening plan in orbit parameters and physical characteristics in order to be classified non-threatening. In order to establish these criteria, three things will have to be considered: the accuracy of surveillance devices in measuring the relevant quantities, the response planned in the event of non-correspondence, and the capability of various nations to make their launched satellites conform to plans. In regard to the latter, it should be possible for a nation to notify the U. S. when it realizes that one of its launches deviates from its plan.

Physical and Behavioral Characteristics

The space defense system will obtain data about detected objects other than orbital. Such characteristics such as mass, size, shape, reflectivity, stabilization, orientation, tumbling rate, and type of rf activity likely will be available. The Physical/Behavioral technique would be a comparison of observed values of these characteristics for a detected satellite with established criteria for non-threatening objects.

This technique rests on the assumption that satellites exhibiting values within a certain range on characteristics observable by the space defense surveillance will be defined by the U. S. to be non-threatening. For instance, a satellite of such low mass that it could not contain a nuclear warhead might be defined as non-threatening. Also, a satellite emitting a gamma ray flux or a neutron flux below a certain threshold which would be exceeded if a nuclear warhead were present might be defined as non-threatening.

Satellites taking actions which are clearly aggressive or preparatory to aggressive actions would be classified as threatening.

The definition of a threatening satellite would have to make explicit what actions are considered aggressive.

In order to select the criteria for this technique, two distributions, one empirical for non-threatening objects and one estimated for threatening objects, would be plotted for each characteristic. Typical plots might be made, for instance, for mass and gamma ray flux density. The two distributions would then be examined to see if some range of the characteristic is more typical of one distribution than the other. If there is such a range, values defining the limits of the range are selected. Any object exhibiting a value in such a range is classified threatening or non-threatening as the case may be.

Authenticating Response to Interrogation

A technique which may be useful in identifying friendly satellites is the Authenticating Response technique. The successful use of this technique consists of an interrogation of the detected satellite by the defense system followed by a prescribed response to the interrogation by the satellite.

Before this technique can be implemented, it has to be decided that available responses are distinctive enough not to be made by chance by a non-friendly satellite, and, more than that, which responses are free from enemy observation or reception and subsequent imitation.

This technique could be implemented by installing an electronic transponder in friendly satellites. These transponders could be interrogated electronically by equipment associated with surveillance radar. This arrangement would be very similar to the IFF of today. Of course, the defense system's receiving equipment would have to be capable of determining that the response was emitted from the satellite in question - a capability which would become more difficult to attain as the number of satellites in orbit increases and as the radius of the orbits increases.

If the defense system's surveillance coverage were continuous, IFF transponders in satellites launched from friendly areas would be superfluous inasmuch as these satellites would be classified non-threatening on the basis of point of launch.

Criteria defining how closely the satellite's response must correspond with the prescribed response will have to be developed.

Sequence of Techniques

If the Authenticating Response technique is implemented by installing an electronic IFF transponder in friendly satellites, it would likely be the first technique applied -- the return from the satellite being received along with radar return. Decoding the return would probably be accomplished in the receiver and hence would require no main computer time.

The Trajectory technique would be used next. The radar return information needed in this technique would require some time to collect, computer time would be required to compute trajectory data from observed data, and computer time would be required to compare trajectory data with stored criteria for non-threatening.

The Correspondence technique would be used next. It would require some amount of time for collecting radar data and computing trajectory data just as the Trajectory technique. However, it would probably require more computer time for comparison with time dependent information in launch and orbit plans than the Trajectory technique would require for comparison with static criteria.

The Physical/Behavioral technique would probably be used last. The information used in this technique would probably not be collected by the continuously operating surveillance devices. The cost of using secondary sensing devices, which might require being put into orbit, would make this the most expensive of the four techniques. It probably would be used only if the other three techniques failed to identify a particular object.

Techniques and Criteria for Raid Recognition

Both raid recognition techniques discussed in Section 2 appear to be possibilities for use against a satellite threat. Conditions under which each could be used are discussed here. It should be noted that the critical weight technique would require considerably more computer time than the critical number technique.

Critical Number

One raid recognition technique which could be used against a satellite threat is the Critical Number technique, in which the number of detected satellites are counted. This number is then compared with the average number of satellites in the system. If the number currently in the system significantly exceeds the average number, it may be assumed at some level of confidence that a raid is in progress.

This technique might be applied to all satellites in orbit or only to those which would be approaching to within missile range of the defended area during the next X minutes. This latter technique would be sensitive to the situation where the total number of unidentified satellites is normal but an abnormally high proportion of them would pass over the defended area nearly simultaneously. If the enemy can choose from alternative tactics which spread out over different time periods the arrival of attack satellites over the defended area, several different values of X might be used.

The critical number technique rests on some assumptions concerning the number of satellites in the system and the number of satellites an enemy would use in a raid. One assumption is that during non-raid conditions the numbers of satellites in the system at different times are approximately normally distributed. If this assumption holds, large deviations from the average number of satellites will be observed less frequently than smaller deviations. This assumption may not hold if break-up of satellites into a large number of fragments becomes a frequent occurrence or if simultaneous launchings of many satellites become as frequent as single launchings. In these cases, the average number of satellites may be exceeded by a large number almost as frequently as by a small number. Hence, a large deviation will not indicate an abnormal condition any more than a small deviation.

The second assumption is that the number of satellites which would be used in any enemy raid significantly exceeds the typical deviation (observed in non-raid conditions) from the average number of detected satellites.

Criteria for this technique would be derived as described in Section 2 using empirical records of numbers of satellites in the system simultaneously or in some period of time. This technique could also be used with number of unidentifiable satellites in the system rather than total number of satellites.

Critical Weight

If this technique were used against a satellite threat, each unidentifiable satellite would be assigned a weight. This weight could reflect the likelihood that the unidentifiable satellite is actually non-threatening or it could reflect the confidence of the defense system in the information available about the satellite. The weights for all unidentifiable satellites would be summed and the sum compared with a "critical weight" to determine if the sum indicates a raid in progress.

From past history, the distribution of values exhibited by non-threatening satellites along trajectory characteristics (such as inclination) and physical characteristics (such as mass) would be available. A satellite exhibiting on such a characteristic a value which had only rarely been exhibited by a non-threatening satellite would receive a large weight.

Past history might also indicate that information from certain surveillance devices, or certain types of information in general, or information obtained under certain conditions is not reliable. When the information about a satellite is of an unreliable quality, the satellite would receive a small weight.

As with the Critical Number technique, this technique might be applied to all satellites in orbit or only to those approaching to within missile range of the defended area during the next X minutes -- X possibly taking on several values.

This implementation of the technique rests on the assumption that during an enemy raid, either (1) the defense system will detect more unidentifiable satellites than during normal conditions or (2) the unidentifiable satellites detected will be weighted higher than during normal conditions.

The criteria for this technique would be derived as described in Section 2 using empirical records of total weights of satellites in the system simultaneously or in some time period.

SECTION 4
SYSTEM DEVELOPMENT STEPS AND GUIDELINES

Initial Development Steps

Six steps can be identified as an approximation to a set of systematic procedures for system development. These steps are appropriate to the early stages of development of an air/space defense system, particularly the early warning functions of identification and raid recognition. The six development steps are defined in this section and guides to their implementation are presented.

The first step is to define system response levels. Available responses must be defined, ordered in terms of several cost/payoff dimensions, and grouped into levels. Responses are classified into two broad categories: responses to individual objects and responses to the overall air/space situation. Within these two response categories, the sequence of implementation of available responses is based on a complex tradeoff between the gains or positively valued payoffs and the costs/risks or negatively valued payoffs associated with each response.

A second step is to define air/space threat levels. Again, two broad classes of threat are defined: threat as a characteristic of individual objects, and as a characteristic of the general air/space environment. In the first threat category, classes of objects which are capable of destructive or otherwise threatening action are defined.

Then, behaviors of such objects which constitute increasing degrees of threat to the area defended by the reference system are defined. In the second threat category, numbers and spatial/temporal densities of threatening objects are defined as levels of threat at an overall situational level.

A third step in system development is to develop and sequence techniques for identification and raid recognition. Based on the definition of threatening objects, the characteristics which discriminate them from non-threatening objects and the information available from the surveillance equipment, techniques are devised for identification. Two types of identification techniques are desirable: those which positively identify threatening objects and those which positively identify non-threats. Techniques for raid recognition are based on information about levels and types of air/space activity which can be defined as significant deviations from normal activity. Degree of deviation is used as an index of confidence in the inference that an attack is in progress.

Step 4 is to reduce to a practical number of categories, the threat continua for individual objects and for the overall air/space situation as defined in Step 2. Level of threat either as a characteristic of an individual object or of an area of air/space is conceptually a continuum. As an object of unknown capability or intent closes with the border of a defended area, threat level increases. Threat level in an area of air/space increases continuously with degrees of deviation from normal levels of activity. The number of meaningful categories of threat is constrained most importantly by the number of identification or raid recognition techniques which can be devised. Beyond this restriction, the number of practical threat categories may be further constrained by the number of system response levels available. This constraint would only apply when the number of response levels was fewer than the number of identification or raid recognition techniques.

A fifth step is to match system response levels to threat levels. The decision of which response level is an appropriate move to counter each threat level reflects policy at a national military level. Where there are more responses than there are specifiable threat levels, the response series can be shifted in one direction or the other to reflect changes in policy. A very militant, aggressive policy would prescribe more harsh responses at low levels of threat than would a more restrained, conciliatory response policy.

Step 6 is to specify criteria for accepting the presence of the threat level tested for by each technique. In the case of identification techniques, information about the detected object is compared either with definitions of threatening or non-threatening objects. Criteria are needed to resolve whether or not the available information is sufficiently close to the definition of threatening or non-threatening to make the assumption that the object is in fact a threat or, in the latter case, a non-threat. Criteria can be made more or less stringent as a function of the consequences of misidentification. The same problem exists in the case of raid recognition techniques: criteria are necessary for accepting the presence of an enemy air/space borne attack.

Table 3 presents this series of system development steps and the classes of information upon which the related decisions are resolved.

TABLE 3

SYSTEM DEVELOPMENT STEPS AND THEIR INFORMATION BASES

Development Steps		Information Bases
Step 1:	Define system response levels	State of the art in U. S.: Defensive weapon technology Offensive weapon technology Surveillance, communication, and data processing technology Command control organization
Step 2:	Define air/space threat levels	Knowledge of enemy: Offensive warheads and carriers Anticipated attack strategies in terms of how many, over what time interval, and spatial distribution
Step 3:	Develop and time sequence identification and raid recognition techniques	State of the art in U. S.: Surveillance technology Communication technology Data processing technology Characteristics of threatening objects and situations which differentiate them from non-threatening objects and situations
Step 4:	Reduce threat levels to a practical number of categories	Threat levels reduced by number not to exceed system response levels or number of techniques
Step 5:	Match system response levels to threat levels	National military policy on a "hard-soft" dimension
Step 6:	Specify criteria for accepting presence of threat levels	Reliability and accuracy of information available Risk involved in rejecting the presence of the threat level if true Cost involved in accepting the presence of the threat level if false

Guides to Step 1: Defining System Response Levels

Response Classes

The kinds of responses potentially available to an air/space defense system for countering threat states are limited primarily by the prevailing states-of-the-art in equipment facilities such as weapons, communication, and surveillance. On the basis of 1950's technology, the following classes of responses could be made to individual aircraft:

1. Gather information about the detected object via the continuously operating elements of the surveillance system.
2. Gather new or additional information about the object via special, non-continuously operating surveillance devices.
3. Maneuver a destructive device within range of the detected object.
4. Communicate to the controller of the detected object a request to reduce his threat status.
5. Destroy the detected object.

Availability of each response to planners of future systems depends in each case on the satisfaction of assumptions concerning the states-of-the-art of related equipment technologies. Each of the five responses was available to the SAGE planners. Key assumptions about capabilities of available equipment could not be met in the case of the anti-missile system, however, and responses 3, 4, and 5 could not be contemplated in NORAD. In a projected satellite vs. satellite environment all five response classes are likely to be available since equipment facilities which permit each response can be assumed.

System responses to the overall air/space threat environment fall into two broad categories as follows:

Defensive Responses

1. Increase level of readiness of the defense system. Levels of readiness can be manipulated separately for portions of a decentralized system and for command control elements independently from weapon elements.

2. Reduce vulnerability of portions of defensive forces.

3. Launch and deploy recallable portions of the defensive weapons to forward areas.

4. Reduce activities of non-military facilities such as air traffic and electromagnetic transmissions.

5. Reduce vulnerability of civilian populations and facilities by moving or sheltering.

6. Engage enemy with defensive forces.

Offensive Responses

1. Increase readiness of portions of retaliatory force.

2. Reduce vulnerability of portions of retaliatory force by hardening or moving.

3. Communicate with representatives of nation suspected of aggressive action.

4. Launch and deploy some recallable portions of the retaliatory force to airborne hold points.

5. Employ retaliatory force against enemy.

Again, the availability of each response depends on an obvious assumption: that the equipment or organizational facilities have the capabilities implied.

Response Levels

Available responses can be grouped into levels on the basis of the costs or risks involved as a consequence of their implementation.

Generally, costs can be used to group responses into four major categories. The highest level category is defined by responses which risk the unwarranted provocation of hostilities. Destroying another nation's aircraft and bombing his territory are obvious examples. Not so obvious are preparatory actions such as sending strategic weapon carriers to airborne holding areas. Actions clearly preparatory to an offensive strike are subject to detection and interpretation by an enemy and may unnecessarily provoke a preventive strike.

A second level of responses is defined by risk of civil panic or undermining civil confidence in the air/space defense system. Actions which control civilian activities and alert the general populace to the dangers of an impending attack are of this class. Such steps would be taken with a reluctance second only to the first level responses and would require very high confidence in the inference that an actual attack was imminent.

A third level of responses is defined by the risks incurred by making certain facilities unavailable for a defined interval of time following their use. Thus, if recallable weapons are launched, held airborne, then must be returned to base, a known period of time necessarily will be required before those weapons can be used again. A similar cost is involved in alerting command and control personnal for emergence duty when in fact no emergency existed.

A fourth and lowest level of cost category is defined by expense of using system facilities. Scrambling interceptors, deploying or hardening strategic weapons, etc. involve dollar costs although they may not include costs of the types defined by the higher three cost categories.

Guides to Step 2: Defining Threat Levels

Definition of threat levels is based principally on information about the capabilities of enemy offensive carriers and warheads. For individual objects, threat is a composite of destructive intent, destructive capability and imminence re: defended areas. An object which does not exhibit all three characteristics can be regarded as non-threatening. Such objects, furthermore, can be regarded as non-threatening for as long as at least one of these three characteristics can be determined to be absent. Currently, there are few (if any) direct means for sensing intent or capability of detected objects; therefore, threat level is primarily based on the one threat dimension for which data can be obtained: imminence. As an object of undetermined intent and/or capability continues to close with U.S. defended areas, threat level is said to increase.

Threat level posed by the overall air/space situation depends upon the number of carriers which would be required to produce unacceptable damage to the U.S., particularly the U.S. retaliatory force. When warhead yields were small, many carriers were required; as yields increase, fewer carriers are needed to pose an equal level of threat. If warhead yields can be infinitely increased over defensive capabilities to render facilities invulnerable to their effects, then a very small number of carriers (aircraft, missiles, satellites) could deliver an unacceptable level of destruction and therefore constitute a definition of threat.

Guides to Step 3: Developing and Sequencing Identification and Raid Recognition Techniques

Constraints on the development of techinques for identification lie principally in two areas. First, in the degree and nature of the differences between threatening and non-threatening objects, e.g. between an armed bomber on a hostile mission and a commercial aircraft; between an experimental or meteorological missile and one containing a nuclear warhead launched toward the U. S. ; between a communications satellite and a missile launching platform. Second, in the capability of surveillance and related data-processing equipment to detect the key differences between the non-threatening and the threatening object. Similarly, constraints on the development of raid recognition techniques depends first on the degree of difference between air/space activity types and levels when an attack is in progress and when it is not; and second, on the capability of sensor systems to detect these differences.

Sequence of application of these techniques depends upon two factors: first, the availability of information required by the technique and second, the efficiency of the technique in terms of reducing the ambiguity of the detected object's threat status. Ideally, techniques which positively identify threats would be used first in a sequence of techniques. These objects are the items of primary interest to the system and their detection permits the application of the second technique which asks, "Does this many threatening objects, in these areas, etc. constitute an attack?" However, depending upon the time order in which information about detected objects becomes available, techniques which positively identify non-threats can be employed to advantage pending information which can be used to test for presence of threat. Techniques which positively identify non-threats are used to remove as many objects as possible from further processing. If available techniques of this type vary in their power to reduce threat ambiguity, then, to reduce the risk of overloading later techniques, the technique should be used first which removes the largest percentage of objects from further processing.

Guides to Step 4: Reducing Threat Levels To a Practical Number of Categories

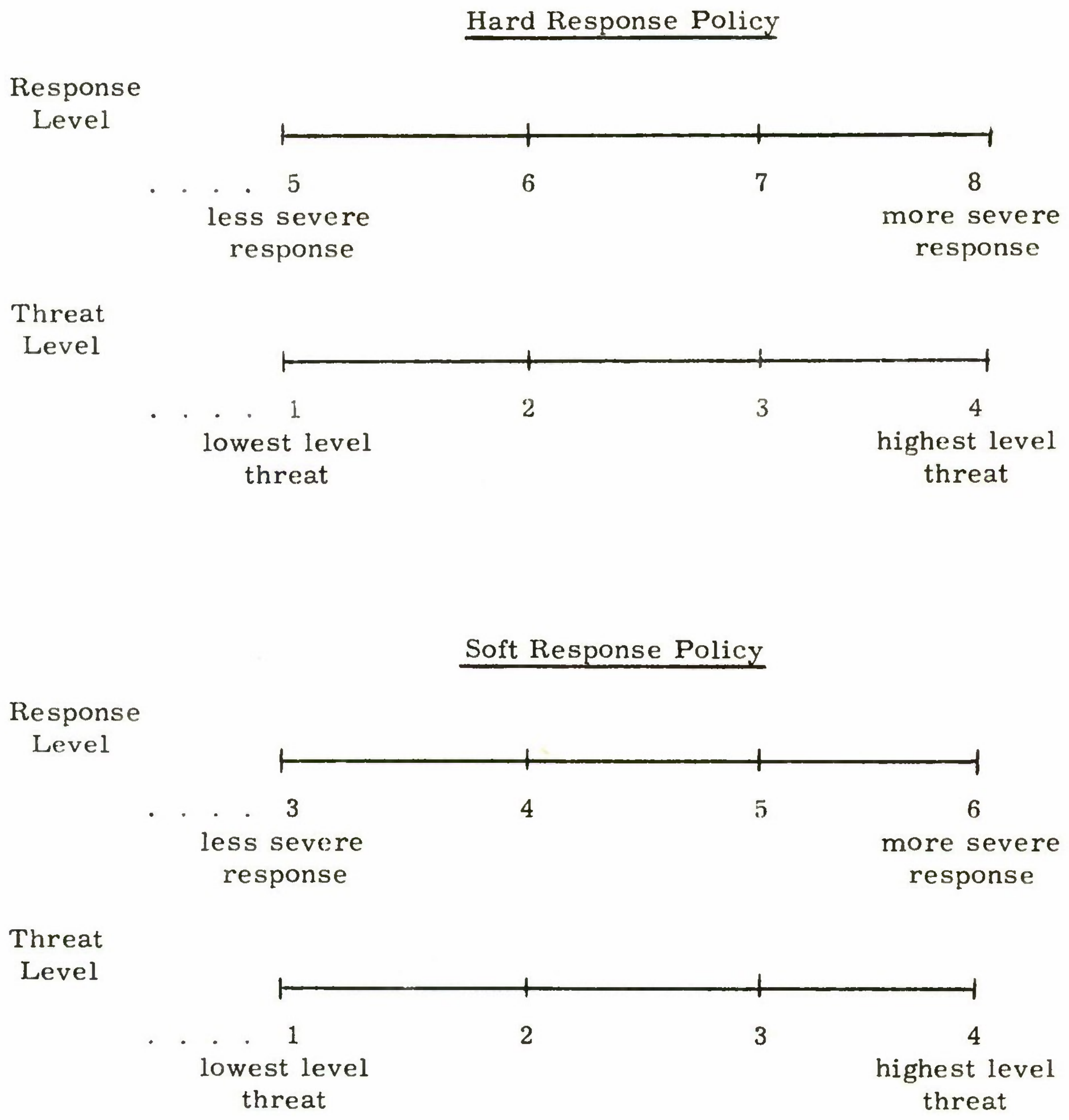
Level or degree of threat posed either by an individual object or by the total complex of air/space activity can be seen as a continuum. An object on a closing course with a U. S. border becomes more threatening by infinitely small degrees as range to the target decreases. Overall threat level similarly increases by infinitely small degrees as more and more signs of corroborative evidence accumulate. These continua must be reduced to a few qualitative categories describing threat levels of significance to the system in terms of required reactions. The actual number of threat categories to be imposed on the underlying threat continuum is first of all a function of the number of techniques which have been developed to test the object or set of objects for threat states, and secondly a function of the number of response levels which can be implemented by the defense system. It is obviously of no value to develop threat state categories when the information which would permit one to know the state existed is not available. Where only a few levels of response are available, there is small value in planning more categories of threat level than there are response levels. Where many gradations of preparedness are potentially available, on the other hand, the number of techniques for determining the existence of different threat levels may place a restraint on the number of practical response levels to plan.

Guides to Step 5: Matching Response Levels to Threat Levels

Once a series of response levels and threat levels are defined, an appropriate matching must be made. The definition of "appropriate" is influenced primarily by policy considerations at a national military level. Various levels of response, more or less severe, could be made to a given threat level and the specific matching could be made sensitive to the prevailing political/military atmosphere. As tensions appear to be relaxing, this trend could be reflected by specifying less severe response sets to each successive threat level. The initial matching and later adjustments would be relatively long term policy decisions rather than day-to-day or even month-to-month tactical decisions. An illustration of the difference between a "soft" and a "hard" response policy in matching response sets to threat levels is presented in Figure 1.

FIGURE 1

MATCHING RESPONSES TO THREAT LEVELS
UNDER "HARD" VS. "SOFT" RESPONSE POLICIES



Hard Response Policy

Soft Response Policy

Guides to Step 6: Specifying Criteria for Accepting Presence of Threat Levels

Each technique for identification or for raid recognition includes criteria for accepting or rejecting the threat state tested for. These criteria can be a formal matter of doctrine or invested in the personal judgment of the military commander. In either case the criteria can be manipulated along a restrictive-permissive continuum. Where along this dimension the criteria for a given threat state are placed, specifies a tradeoff between errors of Type I and Type II. Restrictive criteria reflect the system developer's preference for the risk of rejecting the presence of the threat state when in fact it exists (Type I error), and permissive criteria reflect a preference on the part of the system developer to more often risk accepting the presence of the threat state when it in fact does not exist (Type II error).

The "strictness" or "permissiveness" of the criteria used with a given technique depends upon two considerations: the cost level category of the response planned for the threat state, and the reliability of the available information in discriminating the presence of the threat state.

Responses fall into four cost categories as follows:

Level 1: Risk of precipitating hostilities.

Level 2: Risk of causing civil panic or loss of confidence in warning system.

Level 3: Risk of making certain system facilities unavailable during a time when they might be needed.

Level 4: Expense of using system facilities (fuel, maintenance).

Criteria for accepting the presence of threat states for which actions of cost levels 1 or 2 are planned as the appropriate response are most conservative or restrictive. On the other hand, criteria for accepting the presence of threat states for which cost levels 3 or 4 are planned tend to be less conservative. Responses of levels 1 and 2 are primarily planned for overall threat states which are tested for by raid recognition techniques. Responses of levels 3 and 4 are most typical of those planned for individual object threat states which are tested for by identification techniques.

Criteria are established toward the conservative side of the continuum as a way to compensate for unreliable and incomplete information used by the technique. In general, however, the basic rules appear to be as follows:

> When in doubt, and the response is of low cost (4 or 3), assume the threat state exists and respond appropriately.
>
> When in doubt, and the response is of high cost (2 or1), assume the threat state does not exist and withhold response.

REFERENCES TO THE NATURE OF A SATELLITE THREAT ENVIRONMENT

1. Attridge, W. S., Jr. & Platcow, R. Estimates of enemy technical and operational weapon capabilities-threat model 1965-1970. Lexington, Mass.: The Mitre Corporation, August 1961. (TM-3151) SECRET

2. Conceptual plan--national space surveillance system. Part I Summary. Newport Beach, California: A Division of Ford Motor Company, Aeronutronic, June 1, 1960. (AFCCDD-TR-60-24, Contract No AF 19(604)-6105) SECRET

3. Conceptual plan--national space surveillance system. Part II: System considerations. Newport Beach, California: A Division of Ford Motor Company, Aeronutronic, June 1, 1960. (AFCCDD-TR-60-24, Contract No. AF 19(604)-6105) SECRET

4. Conceptual plan--national space surveillance svstem. Part III: Sensors. Newport Beach, California: A Division of Ford Motor Company, Aeronutronic, June 1, 1960. (AFCCDD-TR-60-24, Contract No. AF 19(604)-6105) SECRET

5. Garfunckel, I. M. Future environments which affect TEAS. Los Angeles, California: Planning Research Corporation, February 1961. SECRET

6. Hughes Aircraft Company. Identification of radiating and non-radiating high altitude vehicles: Phase 1 report. Culver City, California: Author, March 1, 1960. (RADC-TR-60-28, Contract No AF 30(602)-2053, Tack No. 55094) SECRET

7. Hughes Aircraft Company. Identification of the strategic missions of earth satellites. Fullerton, California: Author, November 30, 1960. (AFCRL-TR-60-362, Contract No. AF 19(604)-5871)SECRET

8. Jones, C. M. Proceedings of the conference on recognition of non-cooperative aerospace vehicles. Bedford, Mass.: Air Force Cambridge Research Laboratories, L. G. Hanscom Field, 20-22 September 1960. (AFCRL-TR-60-182) SECRET

9. Radio Corporation of America. Satellite interceptor system study. Volume 1 - system concepts. Burlington, Mass.: Missile Electronics & Controls Division, January 31, 1960. (Final report CR-59-588-39, Contract No. SD-60) SECRET

10. Radio Corporation of America. Satellite interceptor system study. Volume II - subsystems. Burlington, Mass.: Author, January 31, 1960. (Final report CR-59-588-39) SECRET

11. A review of project defender for the director of defense research and engineering. Washington, D. C.: Advanced Research Projects Agency, July 25-29, 1960. (IDA-RESG TR 60-4, Volume 1) SECRET